CORE
Metadata, citation and similar papers at core.ac.uk
Provided by University of Minnesota, Morris (UMM): Digital Well

University of Minnesota Morris Digital Well
University of Minnesota Morris Digital Well

Mathematics Publications | Faculty and Staff Scholarship

7-2007

Fractalized Cyclotomic Polynomials

David P. Roberts
University of Minnesota - Morris, roberts@morris.umn.edu

Follow this and additional works at: https://digitalcommons.morris.umn.edu/mathematics

 Part of the Mathematics Commons

Recommended Citation
David P. Roberts. Fractalized cyclotomic polynomials. *Proceedings of the American Mathematical Society* 135 (2007), no. 7, 1959-1967.

This Article is brought to you for free and open access by the Faculty and Staff Scholarship at University of Minnesota Morris Digital Well. It has been accepted for inclusion in Mathematics Publications by an authorized administrator of University of Minnesota Morris Digital Well. For more information, please contact skulann@morris.umn.edu.

FRACTALIZED CYCLOTOMIC POLYNOMIALS

DAVID P. ROBERTS

ABSTRACT. For each prime power p^m, we realize the classical cyclotomic polynomial $\Phi_{p^m}(x)$ as one of a collection of 3^m different polynomials in $\mathbf{Z}[x]$. We show that the new polynomials are similar to $\Phi_{p^m}(x)$ in many ways, including that their discriminants all have the form $\pm p^c$. We show also that the new polynomials are more complicated than $\Phi_{p^m}(x)$ in other ways, including that their complex roots are generally fractal in appearance.

1. INTRODUCTION

Cyclotomic polynomials $\Phi_d(x)$ and their associated number fields $\mathbf{Q}(e^{2\pi i/d})$ form a substantial topic in algebraic number theory, represented by the books [3] and [7]. Here we restrict attention to the particularly interesting case where the index is a prime power, $d = p^m > 1$. We realize

$$\Phi_{p^m}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = \sum_{j=0}^{p-1} x^{jp^{m-1}} \tag{1.1}$$

as one out of a collection of 3^m different polynomials in $\mathbf{Z}[x]$. Our new polynomials are denoted $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$, where the τ_j are chosen independently from the set $\{0, 1, \infty\}$.

On the one hand, the $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ are very similar to the classical $\Phi_{p^m}(x) = \Phi_{p;1,\ldots,1}(x)$. They have degree $\phi(p^m) = (p-1)p^{m-1}$, are irreducible over the integers, have polynomial discriminant of the form $\pm p^c$, field discriminant equal to their polynomial discriminant, and Galois group having size of the form $(p-1)p^b$. Our proofs of these facts follow classical proofs.

On the other hand, the $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ are in general much more complicated than the classical $\Phi_{p^m}(x)$. Their roots are generally fractal in appearance, rather than intelligibly spaced on a circle. For $p = 2$, there are often many real roots. The Galois groups $\mathrm{Gal}(\Phi_{p;\tau_1,\ldots,\tau_m}(x))$ are typically much larger than $\mathrm{Gal}(\Phi_{p^m}(x)) = (\mathbf{Z}/p^m)^\times$ and moreover highly non-abelian.

Section 2 defines our analogs. Section 3 proves the statements in the second paragraph. Section 4 communicates the complexity of our new polynomials; it draws some root plots, counts real roots, and computes some Galois groups.

For related material we refer the reader as follows. First, the complex roots of our fractalized cyclotomic polynomials $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ are higher circular p-units in the sense of Anderson and Ihara [2]. The general construction of [2] involves iterated covers of the Riemann sphere, $\hat{\mathbf{C}} \stackrel{f_m}{\to} \hat{\mathbf{C}} \stackrel{f_{m-1}}{\to} \cdots \stackrel{f_2}{\to} \hat{\mathbf{C}} \stackrel{f_1}{\to} \hat{\mathbf{C}}$, with each step f_j

2000 *Mathematics Subject Classification.* Primary 11R21; Secondary 12E10, 37F99.
Key words and phrases. cyclotomic, polynomial, discriminant, fractal, Galois.

conjugate by fractional linear transformations to $x \mapsto x^p$ and all critical values of $F_1 \circ \cdots \circ F_m$ in $\{0, 1, \infty\}$. We restrict the allowed fractional linear transformations to the six permuting the cusps $\{0, 1, \infty\}$. Our restriction keeps each f_j defined over $\mathbf{Q}$; it keeps polynomial discriminants, not just field discriminants, of the form $\pm p^c$. Second, our polynomials illustrate the general technique of using iteration to construct infinite extensions of the rationals with only finitely many ramifying primes; [1] provides a general introduction to this technique. Third, our field discriminant formula provides a tool for studying higher ramification subgroups in the infinite extension of $\mathbf{Q}$ obtained by considering all our polynomials belonging to a given fixed prime at once; this application is pursued in the case $p = 2$ in [6].

2. Definition

Let p be a prime. Let $\mathbf{Z}[x]_n$ be the additive group of polynomials in $\mathbf{Z}[x]$ of degree $\leq n$. Define linear operators $R : \mathbf{Z}[x]_n \to \mathbf{Z}[x]_n$ and $F_p : \mathbf{Z}[x]_n \to \mathbf{Z}[x]_{pn}$ by

$$(Rf)(x) = (x-1)^n f\left(\frac{1}{1-x}\right), \tag{2.1}$$

$$(F_p f)(x) = f(x^p). \tag{2.2}$$

A *fractalized cyclotomic polynomial* for the prime p is then by definition any polynomial obtained from $\Phi_p(x) \in \mathbf{Z}[x]_{p-1}$ by successive application of F_p and R in any order. Note that $(F_p^{m-1}\Phi_p)(x) = \Phi_p(x^{p^{m-1}})$ is just the classical cyclotomic polynomial $\Phi_{p^m}(x)$. Inserting R's among the F_p's "fractures" this construction process; this is one reason we use the word "fractalized."

Next, we give a unique name to each fractalized cyclotomic polynomial. As a first step, note that R is related to the map $g_{(01\infty)} : \hat{\mathbf{C}} \to \hat{\mathbf{C}} : x \mapsto 1/(1-x)$. The map $g_{(01\infty)}$ rotates the cusps of $\hat{\mathbf{C}}$, in the sense that $0 \mapsto 1$, $1 \mapsto \infty$, and $\infty \mapsto 0$. One can check that signs have been chosen properly in (2.1) so that R, like $g_{(01\infty)}$, has order three. Thus, using R alone, one can only construct three polynomials from $\Phi_p(x)$. We name them as follows.

$$\Phi_{p;0}(x) = (R\Phi_p)(x) = (-1)^{p-1} \sum_{j=0}^{p-1} \binom{p}{j+1} (-x)^j, \tag{2.3}$$

$$\Phi_{p;1}(x) = \Phi_p(x) = \sum_{j=0}^{p-1} x^j, \tag{2.4}$$

$$\Phi_{p;\infty}(x) = (R^{-1}\Phi_p)(x) = \sum_{j=0}^{p-1} \binom{p}{j} (-x)^j. \tag{2.5}$$

Passing from the summation in (2.4) to the summations in (2.3) and (2.5) is a simple classical computation centering on expanding $(x-1)^p$ by the binomial theorem.

As the second and main step, we bring in F_p. Note that the operator F_p is related to the map $f_p = \hat{\mathbf{C}} \to \hat{\mathbf{C}} : x \mapsto x^p$. To treat 0, 1, and ∞ on an equal

footing, we define degree p maps

$$f_{p;0} = g_{(01\infty)}^{-1} f_p g_{(01\infty)} \quad : \quad x \mapsto 1-(1-x)^p, \tag{2.6}$$

$$f_{p;1} = f_p \quad : \quad x \mapsto x^p, \tag{2.7}$$

$$f_{p;\infty} = g_{(01\infty)} f_p g_{(01\infty)}^{-1} \quad : \quad x \mapsto \frac{x^p}{x^p-(x-1)^p}. \tag{2.8}$$

All three maps fix 0, 1, and ∞. The critical points of $f_{p;\tau}$ are the two points of $\{0,1,\infty\}-\{\tau\}$, each with multiplicity $p-1$. Motivated by this discussion of rational functions, we define

$$F_{p;0} = RF_pR^{-1}, \tag{2.9}$$

$$F_{p;1} = F_p, \tag{2.10}$$

$$F_{p;\infty} = R^{-1}F_pR. \tag{2.11}$$

Henceforth we will emphasize the three operators $F_{p;\tau}$, rather than F_p and R.

Definition 2.1. Let p be a prime, m a positive integer, and $\tau_1, \ldots, \tau_m$ elements of $\{0,1,\infty\}$. Then the corresponding fractalized cyclotomic polynomial $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ is defined by (2.3), (2.4), (2.5) for $m=1$ and by

$$\Phi_{p;\tau_1,\ldots,\tau_m} = F_{p;\tau_m}\cdots F_{p;\tau_2}\Phi_{p;\tau_1}. \tag{2.12}$$

for $m \geq 2$.

By construction, $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ lies in the space $\mathbf{Z}[x]_{\phi(p^m)}$. Clearly, the polynomials $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ just defined exhaust the fractalized cyclotomic polynomials: one cannot get any other polynomials by applying R and F_p iteratively to $\Phi_p(x)$.

There is a basic symmetry among the fractalized cyclotomic polynomials which we have not yet fully incorporated into our formalism. Define $S : \mathbf{Z}[x]_n \to \mathbf{Z}[x]_n$ by $(Sf)(x) = x^n f(1/x)$. Then S is related to the rational map $g_{(0\infty)} : \hat{\mathbf{C}} \to \hat{\mathbf{C}} : x \mapsto 1/x$. In fact, the association $(0\infty) \mapsto g_{(0\infty)}^* = S$ and $(01\infty) \mapsto g_{(01\infty)}^* = R$ extends to an homomorphism $\alpha \mapsto g_\alpha^*$ from S_3 to operators on $\mathbf{Z}[x]_n$. The basic symmetry is then

$$g_\alpha^* \Phi_{p;\tau_1,\ldots,\tau_m} = \Phi_{p;\alpha^{-1}\tau_1,\ldots,\alpha^{-1}\tau_m}. \tag{2.13}$$

Thus the 3^m different $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ fall into the S_3-orbit of $\Phi_{p^m}(x) = \Phi_{p;1,\ldots,1}(x)$, which contains three polynomials, and $(3^m-3)/6$ more S_3-orbits, each with six polynomials.

3. Similarities

The theorem of this paper gives various properties of the fractalized cyclotomic polynomials. All of them are standard in the case of the cyclotomic polynomial $\Phi_{p^m}(x) = \Phi_{p;1,\ldots,1}(x)$. The proofs in the general case consist mostly of applying standard general facts to our situation. To treat ∞ on the same footing as 0 and 1, we define $f(\infty) = a_0$ for $f(x) = a_0x^n + \cdots \in \mathbf{Z}[x]_n$.

Theorem 3.1. *Let p be a prime, m a positive integer, and $\tau_1, \ldots, \tau_m$ elements of $\{0,1,\infty\}$. Let $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ be the corresponding fractalized cyclotomic polynomial. Then*

(Cuspidal values.) *For $\sigma \in \{0, 1, \infty\}$ one has*

$$\Phi_{p;\tau_1,\ldots,\tau_m}(\sigma) = \begin{cases} \pm p & \text{if } \sigma = \tau_1, \\ \pm 1 & \text{if } \sigma \neq \tau_1, \end{cases} \tag{3.1}$$

with all signs positive if p is odd. In particular, $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ has degree $\phi(p^m)$.

(Reduction modulo p.) *Let $\Psi_0(x) = x$, $\Psi_1(x) = -x + 1$, and $\Psi_\infty(x) = -1$. Then*

$$\Phi_{p;\tau_1,\ldots,\tau_m}(x) \equiv \Psi_{\tau_1}(x)^{\phi(p^m)} \text{ modulo } p. \tag{3.2}$$

(Irreducibility.) *$\Phi_{p;\tau_1,\ldots,\tau_m}$ is irreducible in $\mathbf{Z}[x]$.*

(Polynomial discriminant.) *The polynomial discriminant of $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ is $D(\Phi_{p;\tau_1,\ldots,\tau_m}(x)) = \pm p^c$ with*

$$c = p - 2 + \sum_{j=2}^{m} (p-1)^2 p^{j-2} j + \sum_{j=2}^{m} \delta(\tau_1 \neq \tau_j)(p-1)p^{m-j}. \tag{3.3}$$

Here $\delta(\tau_1 \neq \tau_j)$ is 1 if τ_1 and τ_j are different, and otherwise 0.

(Field discriminant.) *The field discriminant of $\mathbf{Q}[x]/\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ is*

$$d(\Phi_{p;\tau_1,\ldots,\tau_m}(x)) = D(\Phi_{p;\tau_1,\ldots,\tau_m}(x)).$$

(Galois group order.) *The Galois group $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ has order of the form $(p-1)p^b$.*

Proof.

Cuspidal values. By inspection of (2.3), (2.4), and (2.5), one sees that (3.1) holds when $m = 1$. In general, our operators preserve cuspidal values up to sign as follows. First, by inspection one has

$$(Rf)(0) = (-1)^n f(1), \qquad (Rf)(1) = (-1)^n f(\infty), \qquad (Rf)(\infty) = f(0). \tag{3.4}$$

Second, clearly $(F_{p,1}f)(\sigma) = \sigma$, for all $\sigma = \{0, 1, \infty\}$. Using $F_{p,0} = RF_{p,1}R^{-1}$ and $F_{p,\infty} = R^{-1}F_{p,1}R^{-1}$ one finds

$$(F_{p;\tau}f)(\sigma) = \begin{cases} (-1)^{(p-1)n} f(\sigma) & \text{if } (\tau,\sigma) = (0,0),\ (0,1),\ (\infty,1),\ (\infty,\infty), \\ f(\sigma) & \text{if } \sigma \neq \tau. \end{cases} \tag{3.5}$$

Here the factor $(-1)^{(p-1)n}$ arises in the first case when a sign $(-1)^n$ enters before the application of F_p and then a second sign $(-1)^{pn}$ enters after the application of F_p. By induction, (3.1) holds for general m, with all signs positive if p is odd.

Reduction modulo p. By inspection of (2.3), (2.4), and (2.5), one sees that the congruence (3.2) holds for $m = 1$. Working in $\mathbf{F}_p[x]$ rather than $\mathbf{Z}[x]$, and considering $\Psi_\tau^n \in \mathbf{F}_p[x]_n$, one has the general formulas $R\Psi_\tau^n = \Psi_{(0\infty 1)\tau}^n$ and $F_p\Psi_\tau^n = \Psi_\tau^{pn}$. These two formulas prove the congruence (3.2) for general m by induction.

Irreducibility. A polynomial $f(x) = a_0x^n + \cdots + a_n$ in $\mathbf{Z}[x]_n$ is called an p-Eisenstein polynomial if and only if

$$\begin{aligned} \mathrm{ord}_p(a_0) &= 0, \\ \mathrm{ord}_p(a_i) &\geq 1 \ \ (1 \leq i \leq n-1), \\ \mathrm{ord}_p(a_n) &= 1. \end{aligned}$$

A general fact about p-Eisenstein polynomials is that they are irreducible in $\mathbf{Z}[x]$, because they are even irreducible in $\mathbf{Z}_p[x]$, where $\mathbf{Z}_p$ is the ring of p-adic integers. If $\tau_1 = 0$, then $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ is p-Eisenstein by the results on cuspidal values and reduction modulo p, hence irreducible. Irreducibility in the case $\tau_1 \neq 0$ then follows by transformation to the $\tau_1 = 0$ case, via (2.13).

Polynomial discriminant. In general, for $f(x) = a_0 x^n + \cdots \in \mathbf{Z}[x]_n$ with roots α_1, $\ldots$, $\alpha_n \in \mathbf{C}$, its discriminant is

$$D(f) = a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2. \tag{3.6}$$

Standard facts about discriminants include its equivariance with respect to fractional linear transformations. In particular,

$$D(g_\alpha^* f) = D(f) \tag{3.7}$$

for $\alpha \in S_3$. Equality (3.7) can be proved directly from the definition (3.6) for the cases $\alpha = (01)$ and $\alpha = (0\infty)$, and the case of general α, including $R = g_{(01\infty)}^*$ then follows. Likewise, a standard fact is $D(F_p f) = \pm p^{np} f(0)^{p-1} f(\infty)^{p-1} D(f)^p$. Combining this fact with (3.4) and (3.7) gives

$$D(F_{p;\tau} f) = \pm p^{np} f(\tau')^{p-1} f(\tau'')^{p-1} D(f)^p, \tag{3.8}$$

where $\{\tau, \tau', \tau''\} = \{0, 1, \infty\}$. For $m = 1$, Equation (3.3) reduces to the known formula $D(\Phi_p) = \pm p^{p-2}$. The general case of (3.3) then follows from induction, using (2.12) and (3.8). In particular, in the expression for $D(F_{p;\tau_j} f)$ given by (3.8) with $f = \Phi_{p;\tau_1,\ldots,\tau_{j-1}}$, one has $\{f(\tau'), f(\tau'')\} = \{\pm 1, \pm 1\}$ if $\tau_j = \tau_1$ and $\{f(\tau'), f(\tau'')\} = \{\pm 1, \pm p\}$ if $\tau_j \neq \tau_1$, by (3.1). In the latter case one gets a contribution of p^{p-1} to $D(F_{p;\tau_j} f)$. In each of the remaining $m - j$ applications of (3.8), this contribution accumulates in the $D(f)$ factor on the right of (3.8), being raised to the p^{th} power each time. This accounts for the term $\delta(\tau_1 \neq \tau_j)(p-1)p^{m-j}$ in (3.3).

Field discriminant. In general, an irreducible polynomial $f(x) \in \mathbf{Z}[x]$ determines a number field $\mathbf{Q}[x]/f(x)$. The discriminant $D(f) \in \mathbf{Z}$ of the polynomial and the discriminant $d(f) \in \mathbf{Z}$ of the field are related by $d(f) = D(f)/i(f)^2$, for $i(f)$ a positive integer. Also, in general, if $f(x)$ is a p-Eisenstein polynomial then $\mathrm{ord}_p(i(f)) = 0$. These generalities apply directly to $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ when $\tau_1 = 0$ and, since $D(\Phi_{p;\tau_1,\ldots,\tau_m}(x))$ has the form $\pm p^c$, yield the equality of the polynomial and field discriminants. Equality in the case $\tau_1 \neq 0$ then follows by transformation to the $\tau_1 = 0$ case, via (2.13).

Galois group size. Let α_m be a complex root of $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$. Inductively define α_{m-1}, $\ldots$, α_1 by $\alpha_{j-1} = f_{p;\tau_j}(\alpha_j)$ so that α_j is a root of $\Phi_{p;\tau_1,\ldots,\tau_j}(x)$. In $\mathbf{C}$, we have the tower of fields $K_j = \mathbf{Q}(\alpha_1, \ldots, \alpha_j)$. We have $K_1 = \mathbf{Q}(e^{2\pi i/p})$ and the p^{th} power of either α_j, $g_{(01\infty)}(\alpha_j)$, or $g_{(01\infty)}^{-1}(\alpha_j)$ is in K_{j-1}. By Kummer theory, for $j = 2$, $\ldots$, m, the extension K_j/K_{j-1} is Galois with group $\mathbf{Z}/p$. Let K_j^g be the Galois closure of K_j. Our discussion shows that each K_j^g/K_1 is Galois with group of order a power of p, and so the Galois group $\mathrm{Gal}(\Phi_{p;\tau_1,\ldots,\tau_m}(x)) = \mathrm{Gal}(K_m^g/\mathbf{Q})$ has order of the form $(p-1)p^b$. □

4. Differences

Root plots. The set $X_{p;\tau_1,\ldots,\tau_m}$ of complex roots of any $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ is easily obtained by iteratively applying the formulas

$$\begin{aligned} X_{p;\tau_1} &= f_{p;\tau_1}^{-1}(\tau_1) - \{\tau_1\}, \\ X_{p;\tau_1,\ldots,\tau_m} &= f_{p;\tau_m}^{-1}(X_{p;\tau_1,\ldots,\tau_{m-1}}) \quad (m \geq 2). \end{aligned}$$

Explicitly, the inverse image operators are given by

$$\begin{aligned} f_{p;0}^{-1}(x) &= \left\{1 - \epsilon(1-x)^{1/p}\right\}, \\ f_{p;1}^{-1}(x) &= \left\{\epsilon x^{1/p}\right\}, \\ f_{p;\infty}^{-1}(x) &= \left\{\frac{1}{1 - \epsilon(1-1/x)^{1/p}}\right\}, \end{aligned}$$

with ϵ running over the p^{th} roots of unity in each case.

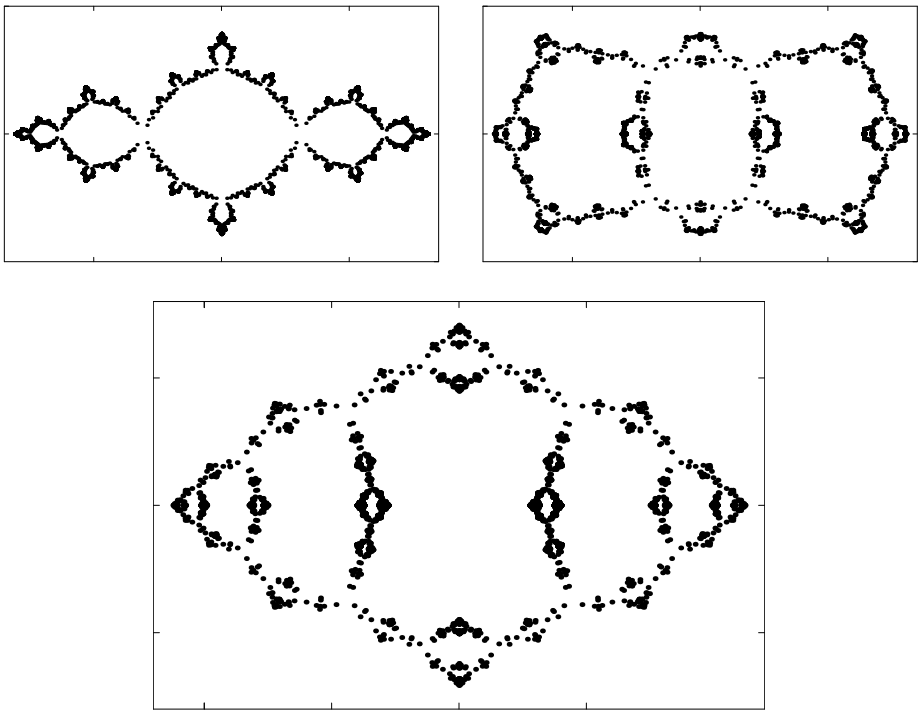

Figure 4.1. Roots of $\Phi_{2;1,0,1,0,1,0,1,0,1,0,1,0,1}(x)$ on the top left and $\Phi_{2;1,0,\infty,0,1,0,\infty,0,1,0,\infty,0,1}(x)$ on the top right, each in the window $[-1.7, 1.7] \times [-1, 1]$ of the complex plane. Roots of $\Phi_{2;1,0,\infty,1,0,\infty,1,0,\infty,1,0,\infty,1}(x)$ on the bottom, drawn to the same scale, now in the larger window $[-2.4, 2.4] \times [-1.6, 1.6]$. There are 4096 roots in each case, with the number of real roots being respectively 2, 338, and 466.

If the last k indices $\tau_{m-k+1}, \ldots, \tau_m$ are all the same, then the root set $X_{p;\tau_1,\ldots,\tau_m}$ is stable under a group μ_{p^k,τ_m} of p^k fractional linear transformations. These transformations take the nicest algebraic form when $\tau_m = 1$, as then they are given by multiplication by p^{kth} roots of unity. Independently, $X_{p;\tau_1,\ldots,\tau_m}$ is invariant under complex conjugation σ. All together, $X_{p;\tau_1,\ldots,\tau_m}$ is stable under a dihedral group $\mu_{p^k,\tau_m} \rtimes \{1, \sigma\}$.

Figure 4.1 shows the roots of three fractalized cyclotomic polynomials with $p = 2$. Figure 4.2 likewise shows the roots of two fractalized polynomials with $p = 3$. In each case we have taken $\tau_m = 1$ and $k = 1$, so the symmetry groups have order 4 and 6 respectively and are clearly visible. The top left image in Figure 4.1 appears commonly in the popular fractal literature, as it approximates the Julia set for the quadratic polynomial $x^2 - 1$.

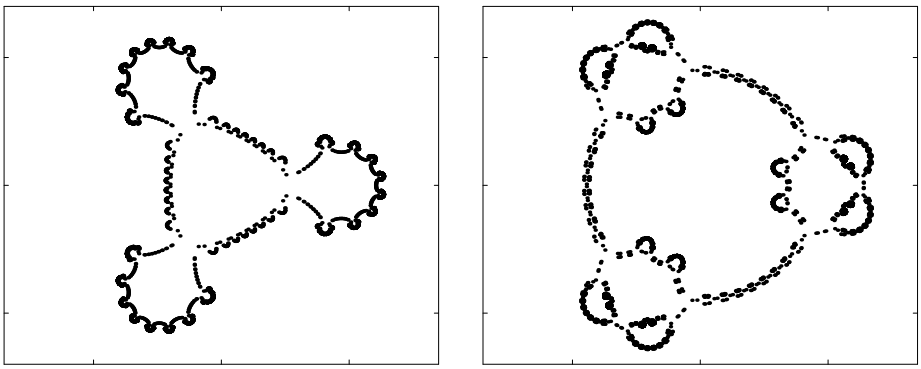

FIGURE 4.2. Roots of $\Phi_{3;1,0,0,1,1,0,0,1}(x)$ on the left and $\Phi_{3;1,0,\infty,1,1,\infty,0,1}$ on the right, each drawn in the window $[-1.7, 1.7] \times [-1.4, 1.4]$, using the same scale as Figure 4.1. Both polynomials here have $\phi(3^8) = 2 \cdot 3^7 = 4374$ roots, all non-real.

Real roots. For $m \geq 2$, the roots of $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ map p-to-1 to the roots of $\Phi_{p;\tau_1,\ldots,\tau_{m-1}}(x)$ under $f_{p;\tau_m}$. The mapping is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant and in particular $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$-equivariant. Thus a root α can be real only if $f_{p;\tau_m}(\alpha)$ is real. If p is odd then no $\Phi_{p;\tau_1,\ldots,\tau_m}(x)$ has real roots simply because no $\Phi_{p;\tau_1}(x)$ has real roots. Henceforth, we restrict to $p = 2$ and derive a simple recursive formula for $s_{\tau_1,\ldots,\tau_m}$, the number of real roots of $\Phi_{2;\tau_1,\ldots,\tau_m}(x)$.

Consider the real circle $\hat{\mathbf{R}} = \mathbf{R} \cup \{\infty\}$ in the Riemann sphere $\hat{\mathbf{C}}$. For $\sigma \in \{0, 1, \infty\}$, let I_σ be the component of $\hat{\mathbf{R}} - \{0, 1, \infty\}$ which does not have σ in its closure. Thus $I_0 = (1, \infty)$, $I_1 = (-\infty, 0)$, and $I_\infty = (0, 1)$. For $\sigma \in \{0, 1, \infty\}$, let $s_{\tau_1,\ldots,\tau_m}(\sigma)$ be the number of roots of $\Phi_{2;\tau_1,\ldots,\tau_m}(x)$ in the interval I_σ. Clearly,

$$s_{\tau_1,\ldots,\tau_m} = \sum_{\sigma \in \{0,1,\infty\}} s_{\tau_1,\ldots,\tau_m}(\sigma). \tag{4.1}$$

In the case $m = 1$, we have $\Phi_{2;0}(x) = x-2$, $\Phi_{2;1}(x) = x+1$, and $\Phi_{2;\infty}(x) = -2x+1$. Thus

$$s_{\tau_1}(\sigma) = \begin{cases} 1 & \text{if } \sigma = \tau_1, \\ 0 & \text{if } \sigma \neq \tau_1. \end{cases} \tag{4.2}$$

So (4.1) recovers the simple fact $s_{\tau_1} = 1$ in all three cases.

Under the map $f_{2;\tau} : \hat{\mathbf{R}} \to \hat{\mathbf{R}}$, an element in I_τ has no preimages. For $\sigma \neq \tau$, an element in I_σ has two preimages, one in I_σ and the other in I_τ. These statements are completely clear in the case of $f_{2;1}$ and then follow for the other two maps. Our discussion proves the following result.

Proposition 4.1. *The number $s_{\tau_1,\ldots,\tau_m}$ of real roots of $\Phi_{2;\tau_1,\ldots,\tau_m}(x)$ is given by (4.1), (4.2), and the recursion*

$$s_{\tau_1,\ldots,\tau_m}(\sigma) = \begin{cases} s_{\tau_1,\ldots,\tau_{m-1}}(\sigma') + s_{\tau_1,\ldots,\tau_{m-1}}(\sigma'') & \text{if } \sigma = \tau_m, \\ s_{\tau_1,\ldots,\tau_{m-1}}(\sigma) & \text{if } \sigma \neq \tau_m, \end{cases}$$

with $\{\sigma, \sigma', \sigma''\} = \{0, 1, \infty\}$.

One can be completely explicit about $s_{\tau_1,\ldots,\tau_m}$ in three special cases as follows. First, note that if $\tau_1 = \tau_2$ then already all three $s_{\tau_1,\tau_1}(\sigma)$ are 0, giving the general formula $s_{\tau_1,\tau_1,\tau_3,\ldots,\tau_m} = 0$. Second, if $\tau_1 \neq \tau_2$ and all the other τ_3, $\ldots$, τ_m are in $\{\tau_1, \tau_2\}$ then inductively one has $s_{\tau_1,\ldots,\tau_m} = 2$. This case is represented by the upper left plot in Figure 4.1. Third, suppose that $\tau_1 \neq \tau_2$ and each index τ_3, $\ldots$, τ_m is taken to be the unique index different from its two immediate predecessors. Then inductively for $m \geq 2$ one has $s_{\tau_1,\ldots,\tau_m} = 2s_{\tau_1,\ldots,\tau_m}(\tau_m) = 2F_m$, where the F_m is the m^{th} Fibonacci number.

In fact, Fibonacci-like behavior can be seen in the root plot of any $\Phi_{2;\tau_1,\ldots,\tau_m}(x)$ having real roots. For example, if $\tau_m = 1$ then by the $x \mapsto -x$ symmetry, the number of roots in $(-\infty, 0)$ is equal to the number of roots in $(0, 1)$ plus the number of roots in $(1, \infty)$. In the three plots in Figure 4.1, this equation is $1 = 0 + 1$, $169 = 70 + 99$, and $233 = 144 + 89$.

Galois groups. The Galois group of $\Phi_{p^m}(x)$ is the group $(\mathbf{Z}/p^m)^\times$, of order $\phi(p^m) = (p-1)p^{m-1}$. While in general $G = \mathrm{Gal}(\Phi_{p;\tau_1,\ldots,\tau_m}(x))$ also has order of the form $(p-1)p^b$, computation shows that the isomorphism type of G and even its order can depend subtly on the indices τ_1, $\ldots$, τ_m.

General theorems give one some control over the possibilities for G. For example, for $p = 2$ the result of [4] says that a finite Galois 2-extension of $\mathbf{Q}$ ramified at 2 only has Galois group generated by complex conjugation and a single other element. So while the Sylow 2-subgroup P of $S_{2^{m-1}}$ has size $2^{2^{m-1}-1}$, any $\mathrm{Gal}(\Phi_{2;\tau_1,\ldots,\tau_m}(x))$ must be smaller when $m \geq 4$, as P requires $m-1$ elements to generate it.

$\tau_1\tau_2\tau_3\tau_4$	$\mathrm{ord}_2(\lvert G\rvert)$	G	$\tau_1\tau_2\tau_3\tau_4$	$\mathrm{ord}_2(\lvert G\rvert)$	G
aaaa	3	$T2$	*abac*	6	$T28$
aaab	5	$T21$	*abba*	6	$T30$
aaba	5	$T19$	*abbb*	4	$T8$
aabb	5	$T17$	*abbc*	6	$T28$
aabc	4	$T6$	*abca*	6	$T27$
abaa	4	$T8$	*abcb*	6	$T27$
abab	6	$T30$	*abcc*	5	$T16$

TABLE 4.1. Galois groups $G = \mathrm{Gal}(\Phi_{2;\tau_1,\ldots,\tau_4}(x))$, with a, b, and c representing distinct elements of $\{0, 1, \infty\}$.

Table 4.1 presents all possibilities for the case $(p, m) = (2, 4)$ of octic polynomials. Galois groups were computed using [5], with Tn indicating that G is the n^{th} group on the standard list of fifty octic groups. A much more elaborate computation for $(p, m) = (2, 5)$ found that while $\text{ord}_2(|G|)$ is 4 in the cyclotomic case, it ranges from 6 to 11 in the forty other cases, with in total twenty-eight isomorphism classes of degree 16 permutation groups G represented. This situation for general (p, m) is quite unusual for Galois theory, as one has a collection of explicit polynomials but no generic expectation for their Galois groups.

References

[1] Wayne Aitken, Farhsid Hajir, Christian Maire, *Finitely ramified iterated extensions.* Int. Math. Res. Not. **2005**, no. 14, 855-880. MR2146860

[2] Greg W. Anderson, Yasutaka Ihara, *Pro-ℓ branching coverings of $\mathbf{P}^1$ and higher circular ℓ-units,* Ann. of Math. **128** (1988), no. 2, 271-293. MR0960948 (89f:14023)

[3] Serge Lang, *Cyclotomic fields I and II. Combined second edition. With an appendix by Karl Rubin,* Graduate Texts in Mathematics, 121, Springer-Verlag, New York, 1990. xviii + 433pp. MR1029028 (91c:11001)

[4] G. N. Markšaĭtis, *On p-extensions with one critical number (Russian)*, Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963), 463-466. MR0151452 (27 #1427)

[5] PARI/GP, Version 2.1.5, Bordeaux, 2004, `http://pari.math.u-bordeaux.fr/`.

[6] David P. Roberts, 2-*adic ramification in some* 2-*extensions of* $\mathbf{Q}$, in preparation.

[7] Lawrence C. Washington, *Introduction to cyclotomic fields. Second edition,* Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997. xiv + 487pp. MR1421575 (97h:11130)

Division of Science and Mathematics, University of Minnesota-Morris, Morris, MN 56267

E-mail address: `roberts@morris.umn.edu`